Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.1.2.A1 Verwendung von grundlegenden Sicherheitsmechanismen (B)

Der eingesetzte Webbrowser MUSS sicherstellen, dass jede Instanz und jeder Verarbeitungsprozess nur auf die eigenen Ressourcen zugreifen kann (Sandboxing). Webseiten MÜSSEN als eigenständige Prozesse oder mindestens als eigene Threads voneinander isoliert werden. Plug-ins und Erweiterungen MÜSSEN ebenfalls in isolierten Bereichen ausgeführt werden.

Der verwendete Webbrowser MUSS die Content Security Policy (CSP) umsetzen. Der aktuell höchste Level der CSP SOLLTE erfüllt werden.

Der Browser MUSS Maßnahmen zur Same-Origin-Policy und Subresource Integrity unterstützen.

APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation (B)

Der Webbrowser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Verbindungen zu Webservern MÜSSEN mit TLS verschlüsselt werden, falls dies vom Webserver unterstützt wird. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Webbrowser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797 unterstützen und einsetzen.

APP.1.2.A3 Verwendung von vertrauenswürdigen Zertifikaten (B)

Falls der Webbrowser eine eigene Liste von vertrauenswürdigen Wurzelzertifikaten bereitstellt, MUSS sichergestellt werden, dass nur der IT-Betrieb diese ändern kann. Falls dies nicht durch technische Maßnahmen möglich ist, MUSS den Benutzenden verboten werden, diese Liste zu ändern. Außerdem MUSS sichergestellt werden, dass der Webbrowser Zertifikate lokal widerrufen kann.

Der Webbrowser MUSS die Gültigkeit der Server-Zertifikate mithilfe des öffentlichen Schlüssels und unter Berücksichtigung des Gültigkeitszeitraums vollständig prüfen. Auch der Sperrstatus der Server-Zertifikate MUSS vom Webbrowser geprüft werden. Die Zertifikatskette einschließlich des Wurzelzertifikats MUSS verifiziert werden.

Der Webbrowser MUSS den Benutzenden eindeutig und gut sichtbar darstellen, ob die Kommunikation im Klartext oder verschlüsselt erfolgt. Der Webbrowser SOLLTE den Benutzenden auf Anforderung das verwendete Serverzertifikat anzeigen können. Der Webbrowser MUSS den Benutzenden signalisieren, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Der Webbrowser MUSS in diesem Fall die Verbindung abbrechen, bis die Benutzenden diese ausdrücklich bestätigt haben.

APP.1.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.2.A6 Kennwortmanagement im Webbrowser (B)

Wird ein Kennwortmanager im Webbrowser verwendet, MUSS er eine direkte und eindeutige Beziehung zwischen Webseite und hierfür gespeichertem Kennwort herstellen. Der Kennwortspeicher MUSS die Passwörter verschlüsselt speichern. Es MUSS sichergestellt werden, dass auf die im Kennwortmanager gespeicherten Passwörter nur nach Eingabe eines Master-Kennworts zugegriffen werden kann. Außerdem MUSS sichergestellt sein, dass die Authentisierung für den kennwortgeschützten Zugriff nur für die aktuelle Sitzung gültig ist.

Der IT-Betrieb MUSS sicherstellen, dass der verwendete Browser den Benutzenden die Möglichkeit bietet, gespeicherte Passwörter zu löschen.

APP.1.2.A13 Nutzung von DNS-over-HTTPS (B)

Die Institution MUSS entscheiden, ob die verwendeten Browser DNS-over-HTTPS (DoH) verwenden sollen. Die Browser MÜSSEN entsprechend dieser Entscheidung konfiguriert werden.

Falls ein interner DNS-Resolver verwendet wird, MUSS dieser auch vom Browser verwendet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.1.2.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.2.A7 Datensparsamkeit in Webbrowsern (S) [Benutzende]

Cookies von fremden Institutionen SOLLTEN im Webbrowser abgelehnt werden. Gespeicherte Cookies SOLLTEN durch die Benutzenden gelöscht werden können.

Die Funktion zur Autovervollständigung von Daten SOLLTE deaktiviert werden. Wird die Funktion dennoch genutzt, SOLLTEN die Benutzenden diese Daten löschen können. Die Benutzenden SOLLTE außerdem die Historiendaten des Webbrowsers löschen können.

Sofern vorhanden, SOLLTE eine Synchronisation des Webbrowsers mit Cloud-Diensten deaktiviert werden. Telemetriefunktionen sowie das automatische Senden von Absturzberichten, URL-Eingaben und Sucheingaben aus der Institution heraus oder an Externe SOLLTEN soweit wie möglich deaktiviert werden.

Peripheriegeräte wie Mikrofon oder Webcam sowie Standortfreigaben SOLLTEN nur für Webseiten aktiviert werden, bei denen sie unbedingt benötigt werden. Der Browser SOLLTE eine Möglichkeit bieten, WebRTC, HSTS und JavaScript zu konfigurieren bzw. abzuschalten.

APP.1.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.1.2.A9 Einsatz einer isolierten Webbrowser-Umgebung (H)

Die Institution SOLLTE speziell abgesicherte, isolierte Browserumgebungen einsetzen, wie z. B. ReCoBS oder virtualisierte Instanzen.

APP.1.2.A10 Verwendung des privaten Modus (H) [Benutzende]

Der Webbrowser SOLLTE bei erhöhten Anforderungen bezüglich der Vertraulichkeit im sogenannten privaten Modus ausgeführt werden, sodass keine Informationen oder Inhalte dauerhaft auf dem IT-System der Benutzenden gespeichert werden. Der Browser SOLLTE so konfiguriert werden, dass lokale Inhalte beim Beenden gelöscht werden.

APP.1.2.A11 Überprüfung auf schädliche Inhalte (H)

Aufgerufene Internetadressen SOLLTEN durch den Webbrowser auf potenziell schädliche Inhalte geprüft werden. Der Webbrowser SOLLTE die Benutzenden warnen, wenn Informationen über schädliche Inhalte vorliegen. Eine als schädlich klassifizierte Verbindung SOLLTE NICHT aufgerufen werden können. Das verwendete Verfahren zur Überprüfung DARF NICHT gegen Datenschutz- oder Geheimschutz-Vorgaben verstoßen.

APP.1.2.A12 Zwei-Browser-Strategie (H)

Für den Fall von ungelösten Sicherheitsproblemen mit dem verwendeten Webbrowser SOLLTE ein alternativer Browser mit einer anderen Plattform installiert sein, der den Benutzenden als Ausweichmöglichkeit dient.

4. Weiterführende Informationen

4.1. Wissenswertes

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 047: „Absicherungsmöglichkeiten beim Einsatz von Webbrowsern"
- Mindeststandard des BSI für den Einsatz des SSL/ TLS-Protokoll durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG
- Mindeststandard des BSI für Webbrowser nach § 8 Absatz 1 Satz 1 BSIG
- Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS): BSI-PP-0040

Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.1.4 Mobile Anwendungen (Apps)

1. Beschreibung

1.1. Einleitung

Smartphones, Tablets und ähnliche mobile Geräte sind heute auch in Behörden und Unternehmen weit verbreitet. Mitarbeitende können so unabhängig von Ort und Zeit auf Daten der Institution, auf Informationen und Anwendungen zugreifen.

Mobile Anwendungen (Applikationen, kurz Apps) sind Anwendungen, die auf mobil genutzten Betriebssystemen wie iOS oder Android auf entsprechenden Endgeräten installiert und ausgeführt werden. Apps werden üblicherweise aus sogenannten App Stores bezogen. Diese werden oft von den herstellenden Institutionen der mobil genutzten Betriebssysteme und Endgeräte betrieben und gepflegt. Im professionellen Umfeld ist es aber auch üblich, Apps selbst zu entwickeln und z. B. über Mobile-Device-Management-Lösungen (MDM) auf den Endgeräten zu installieren und zu verwalten. Im Vergleich zu Anwendungen auf Desktop-Betriebssystemen unterliegen Apps unter iOS oder Android besonderen Rahmenbedingungen, wie etwa einem durch das Betriebssystem sichergestellten Berechtigungsmanagement.

Für die unterschiedlichen mobilen Betriebssysteme gibt es mittlerweile eine große Auswahl an verfügbaren Apps. Auch gibt es standardisierte Bibliotheken und Entwicklungsumgebungen, mit deren Hilfe sich Apps im Vergleich zu klassischen Anwendungen schnell selbst entwickeln lassen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die auf mobilen Endgeräten mit Apps verarbeitet werden. Auch die Einbindung von Apps in eine bestehende IT-Infrastruktur wird dabei betrachtet. Der Baustein definiert zudem Anforderungen, um Apps richtig auszuwählen und sicher betreiben zu können. Dabei werden die Apps unabhängig von ihrer Quelle (App Store oder eigene Installation) betrachtet.

1.3. Abgrenzung und Modellierung

Der Baustein APP.1.4 *Mobile Anwendungen (Apps)* ist auf alle Anwendungen anzuwenden, die auf mobilen Endgeräten eingesetzt werden.

Der Baustein betrachtet Apps unter mobilen Betriebssystemen wie iOS und Android. Anforderungen, welche die zugrundeliegenden Betriebssysteme betreffen, werden hier nicht berücksichtigt. Diese Anforderungen finden sich beispielsweise in den Bausteinen SYS.3.2.3 *iOS (for Enterprise)* sowie SYS.3.2.4 *Android*. Oft werden Apps zentral über ein Mobile Device Management verwaltet. Anforderungen hierzu können dem Baustein SYS.3.2.2 *Mobile Device Management (MDM)* entnommen werden.

Ebenso sind anwendungsspezifische Aspekte von Apps nicht Gegenstand des Bausteins zu mobilen Anwendungen. Diese werden in den entsprechenden Bausteinen der Schicht APP *Anwendungen, wie z. B.* APP.1.2 *Webbrowser* behandelt.

Apps greifen häufig auf Backend-Systeme oder Server bzw. Anwendungsdienste zurück. Werden die Backend-Systeme oder Server selber betrieben, werden Sicherheitsempfehlungen dazu nicht an dieser Stelle gegeben, sondern in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums. Dazu gehören beispielsweise APP.3.1 *Webanwendungen und Webservices* oder APP.4.3 *Relationale Datenbanken*. Zusätzlich sollten die Bausteine berücksichtigt werden, die sich mit allgemeinen Aspekten von Anwendungen befassen, etwa OPS.1.1.6 *Software-Tests und -Freigaben* oder APP.6 *Allgemeine Software*, da diese Aspekte nicht im vorliegenden Baustein berücksichtigt werden. Bei der Entwicklung eigener Apps sollten die Anforderungen des Bausteins CON.8 *Software-Entwicklung* berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.1.4 *Mobile Anwendungen (Apps)* von besonderer Bedeutung.

2.1. Ungeeignete Auswahl von Apps

Die ausgewählten Apps wirken sich stark auf die damit verarbeiteten Informationen, auf das mobile Endgerät sowie häufig auf die IT-Infrastruktur der Institution aus. Wird dies bei der Auswahl der Apps nicht berücksichtigt, können weitreichende Probleme entstehen. Besonders hoch ist die Gefahr, wenn es sich dabei um Apps handelt, die nicht eigens für die abzubildenden Geschäftsprozesse entwickelt wurden. So könnten beispielsweise die für den Betrieb einer App erforderlichen Voraussetzungen nicht ausreichend betrachtet werden. Möglicherweise ist dann z. B. die mobile Netzanbindung nicht leistungsfähig genug oder die Hardware nicht kompatibel. Apps können auch dann ungeeignet sein, wenn sie keine ausreichende langfristige Einsatzstabilität und -planung bieten oder von den herstellenden Institutionen nicht ausreichend gepflegt werden.

2.2. Zu weitreichende Berechtigungen

Apps benötigen gewisse Berechtigungen, um auf bestimmte Funktionen und Dienste zugreifen zu können. So kann eine App in der Regel immer auf die Internetverbindung des mobilen Endgeräts zugreifen. Der Standort oder das Adressbuch müssen hingegen meist gesondert freigegeben werden. Werden Apps eingesetzt, die zu weitgehende Berechtigungen erfordern, oder werden die Berechtigungen nicht ausreichend eingeschränkt, so kann sich das insbesondere auf die Vertraulichkeit und Integrität der Informationen auf dem Endgerät auswirken. Apps können zudem Informationen an unberechtigte Dritte weitergeben, wie z. B. den Standort, Fotos oder Kontakt- und Kalenderdaten. Außerdem sind Apps in der Lage, lokal abgespeicherte Daten zu verändern oder zu löschen. Schließlich können Apps auch Kosten verursachen, etwa durch Telefonanrufe, versendete SMS oder In-App-Käufe.

2.3. Ungewollte Funktionen in Apps

Zwar prüfen manche App-Store-Betreibende die angebotenen Apps, dennoch können diese Sicherheitslücken oder bewusst eingesetzte Schadfunktionen enthalten. Das Risiko ist insbesondere dann hoch, wenn Apps aus ungeprüften oder unzuverlässigen Quellen bezogen werden. Dann kann die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gefährdet werden.

2.4. Software-Schwachstellen und Fehler in Apps

Apps können Schwachstellen enthalten, über die sie direkt am Gerät oder über Netzverbindungen angegriffen werden können. Außerdem werden viele Apps nach einiger Zeit von den Entwickelnden nicht mehr weiter gepflegt. Dadurch werden erkannte Sicherheitsmängel nicht mehr durch entsprechende Updates behoben.

2.5. Unsichere Speicherung lokaler Anwendungsdaten

Einige Apps speichern Daten auf dem Endgerät, beispielsweise Profile der Benutzenden oder Dokumente. Falls diese Daten unzureichend geschützt sind, können möglicherweise andere Apps darauf zugreifen. Dies betrifft neben bewusst abgelegten Daten auch temporäre Daten, wie beispielsweise im Cache zwischengespeicherte Informationen. Auch sind sie für Unberechtigte leicht lesbar, z. B. wenn Mitarbeitende ihre Geräte verloren haben. Außerdem werden lokal gespeicherte Informationen oft nicht im Datensicherungskonzept berücksichtigt. Fällt das Endgerät aus oder geht verloren, sind die lokal gespeicherten Informationen ebenfalls nicht mehr verfügbar.

2.6. Ableitung vertraulicher Informationen aus Metadaten

Durch Apps sammeln sich viele Metadaten an. Mithilfe dieser Metadaten können Dritte auf vertrauliche Informationen schließen, z. B. über Telefon- und Netzverbindungen, Bewegungsdaten oder besuchte Webseiten. Daraus lassen sich dann weitere Informationen ableiten, beispielsweise die Organisationsstruktur der Institution, genaue Positionen von Standorten sowie deren personelle Besetzung.

2.7. Abfluss von vertraulichen Daten

Daten werden über verschiedene Wege von und zu einer App übertragen. Dafür stellen mobile Betriebssysteme verschiedene Schnittstellen bereit. Benutzende haben ebenfalls verschiedene Möglichkeiten, Daten mit einer App auszutauschen, etwa lokal über eine Speicherkarte, die Zwischenablage, die Gerätekamera oder andere Anwendungen. Außerdem können Daten über Cloud-Dienste oder Server der App- oder Geräte-anbietenden Institution übertragen werden. Darüber können Dritte Zugriff auf die vertraulichen Daten erlangen. Schließlich kann auch das Betriebssystem selbst Daten für den schnelleren Zugriff zwischenspeichern (Caching). Dabei können Daten versehentlich abfließen oder Angreifende auf vertrauliche Informationen zugreifen.

2.8. Unsichere Kommunikation mit Backend-Systemen

Viele Apps kommunizieren mit Backend-Systemen, über die Daten mit dem Datennetz der Institution ausgetauscht werden. Die Daten werden bei mobilen Geräten zumeist über unsichere Netze wie ein Mobilfunknetz oder WLAN-Hotspots übertragen. Werden für die Kommunikation mit Backend-Systemen aber unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden.

2.9. Kommunikationswege außerhalb der Infrastruktur der Institution

Wenn Apps unkontrolliert mit Dritten kommunizieren können, kann dies Kommunikationswege schaffen, die nicht von der Institution erkannt und kontrolliert werden können. So können Benutzende beispielsweise die App eines Cloud-Datenspeicherdienstes nutzen, um Informationen vom Endgerät nach außen zu übertragen. Auch die enge Verzahnung von Social-Media-Diensten mit vielen Apps erschwert die Kontrolle, ob und wie Informationen das Endgerät verlassen. Diese Art von Kommunikationswegen ist nur schwer nachzuvollziehen. Dies kann noch weitere Probleme verursachen, etwa wenn Informationen oder Vorgänge archiviert werden müssen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.4 *Mobile Anwendungen (Apps)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.1.4.A1 Anforderungsanalyse für die Nutzung von Apps (B) [Fachverantwortliche]

In der Anforderungsanalyse MÜSSEN insbesondere Risiken betrachtet werden, die sich aus der mobilen Nutzung ergeben. Die Institution MUSS prüfen, ob ihre Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumgebung mobiler Endgeräte ausreichend sind, um sie sicher nutzen zu können.

APP.1.4.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen (B) [Fachverantwortliche]

Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so fixiert werden, dass sie nicht durch Personen oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

Bevor eine App in einer Institution eingeführt wird, MUSS sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen MÜSSEN hinterfragt und gegebenenfalls unterbunden werden.

APP.1.4.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A7 Sichere Speicherung lokaler App-Daten (B)

Wenn Apps auf interne Dokumente der Institution zugreifen können, MUSS sichergestellt sein, dass die lokale Datenhaltung der App angemessen abgesichert ist. Insbesondere MÜSSEN Zugriffsschlüssel verschlüsselt abgelegt werden. Außerdem DÜRFEN vertrauliche Daten NICHT vom Betriebssystem an anderen Ablageorten zwischengespeichert werden.

APP.1.4.A8 Verhinderung von Datenabfluss (B)

Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Profile über die Benutzenden erstellt werden, MUSS die App-Kommunikation geeignet eingeschränkt werden. Dazu SOLLTE die Kommunikation im Rahmen des Test- und Freigabeverfahrens analysiert werden. Weiterhin SOLLTE überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.1.4.A3 Verteilung schutzbedürftiger Apps (S)

Interne Apps der Institution und Apps, die schutzbedürftige Informationen verarbeiten, SOLLTEN über einen institutionseigenen App Store oder via MDM verteilt werden.

APP.1.4.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.1.4.A12 Sichere Deinstallation von Apps (S)

Werden Apps deinstalliert, SOLLTEN auch Daten gelöscht werden, die auf externen Systemen, beispielsweise bei den App-Anbietenden, gespeichert wurden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.1.4.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.1.4.A14 Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps (H)

Falls möglich, SOLLTE für die Authentisierung in Apps ein zweiter Faktor benutzt werden. Hierbei SOLLTE darauf geachtet werden, dass eventuell benötigte Sensoren oder Schnittstellen in allen verwendeten Geräten vorhanden sind. Zusätzlich SOLLTE bei biometrischen Verfahren berücksichtigt werden, wie resistent die Authentisierung gegen mögliche Fälschungsversuche ist.

APP.1.4.A15 Durchführung von Penetrationstests für Apps (H)

Bevor eine App für den Einsatz freigegeben wird, SOLLTE ein Penetrationstest durchgeführt werden. Dabei SOLLTEN alle Kommunikationsschnittstellen zu Backend-Systemen sowie die lokale Speicherung von Daten auf mögliche Sicherheitslücken untersucht werden. Die Penetrationstests SOLLTEN regelmäßig und zusätzlich bei größeren Änderungen an der App wiederholt werden.

APP.1.4.A16 Mobile Application Management (H)

Falls möglich, SOLLTE für das zentrale Konfigurieren von dienstlichen Apps ein Mobile Application Management verwendet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) stellt mit dem Leitfaden „Apps & Mobile Services – Tipps für Unternehmen“ (2. Auflage, 2014) eine Entscheidungshilfe zum Thema Apps und Mobile Services in Unternehmen bereit.

Das Information Security Forum (ISF) bietet eine Broschüre mit dem Titel „Securing Mobile Apps – Embracing mobile, balancing control“ (2018) an.

Auch die „NIST Special Publication 800-163: Vetting the Security of Mobile Applications“ (2015) bietet weiterführende Informationen zum Thema Apps.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.1 Allgemeiner Verzeichnisdienst

1. Beschreibung

1.1. Einleitung

Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Kennung der Name und Vorname des oder der Benutzenden, die Personalnummer und der Name des IT-Systems abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen
- Benutzendenverwaltung, z. B. zur Verwaltung von Konten und Berechtigungen
- Bereitstellung eines Backend-Dienstes für Authentifizierungsfunktionen, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise vorwiegend abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.

Wenn ein Verzeichnisdienst eingesetzt wird, können manche Verwaltungsaufgaben innerhalb des Netzes, wie z. B. Kontenerstellung, Passwortänderungen und Zuweisungen von Rollen und Gruppen, an zentraler Stelle durchgeführt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* ist für alle verwendeten Verzeichnisdienste anzuwenden.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte gibt es im IT-Grundschutz-Kompendium weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind. Bausteine zu Server-Betriebssystemen, auf denen Verzeichnisdienste üblicherweise betrieben werden, sind in der Schicht SYS.1 *Server* des IT-Grundschutz-Kompendiums aufgeführt. Grundlegende Anforderungen an Software-Produkte finden sich in APP.6 *Allgemeine Software* und sind ebenfalls zu beachten.

Verzeichnisdienste sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung,* OPS.1.2.5 *Fernwartung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mitberücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit von Verzeichnisdiensten stützt sich stark auf die Sicherheit des Basisbetriebssystems und dabei vor allem auf die Dateisystemsicherheit. Verzeichnisdienste lassen sich auf vielen Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse über das jeweilige Betriebssystem voraus. Sollte die entstehende Gesamtlösung sehr heterogen oder komplex sein, kann ein nicht ausreichend geplanter Einsatz des Verzeichnisdienstes im Wirkbetrieb zu Sicherheitslücken führen.

2.2. Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Durch eine Partitionierung können die Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen) aufgeteilt werden. Um für eine bessere Lastverteilung zu sorgen, werden Partitionen des Verzeichnisdienstes häufig auf weitere Instanzen repliziert. Außerdem wird durch die redundante Datenhaltung die Ausfallsicherheit verbessert und somit die Verfügbarkeit erhöht. Von entscheidender Bedeutung ist deshalb auch hier eine geeignete Planung, da Partitions- und Replikationseinstellungen zwar nachträglich geändert werden können, dies aber Probleme verursachen kann. Es kann etwa zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Ausfällen führen.

2.3. Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die durchzuführenden Aufgaben erforderlich sind. Dies gilt auch für die Berechtigungen, die über einen Verzeichnisdienst verwaltete Benutzende und Gruppen erhalten, auch wenn diese für die Informationen *im* Verzeichnisdienst selbst gelten. Werden diese Rechte fehlerhaft administriert, kann einerseits der Betrieb gestört werden, falls erforderliche Rechte nicht zugewiesen wurden. Andererseits können Sicherheitslücken entstehen, falls über die notwendigen Rechte hinaus weitere Rechte vergeben werden. Wenn die Zugriffsrechte im Verzeichnisdienst falsch oder inkonsistent vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Ein besonders kritischer Punkt sind auch die Administrationsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept unterlaufen oder unter Umständen sogar die Administration des Verzeichnissystems selbst verhindert oder eine unberechtigte Nutzung ermöglicht werden.

2.4. Fehlerhafte Konfiguration des Zugriffs auf Verzeichnisdienste

In vielen Fällen müssen weitere Applikationen wie Internet- oder Intranet-Anwendungen auf den Verzeichnisdienst zugreifen. Eine Fehlkonfiguration kann dazu führen, dass Zugriffsrechte falsch vergeben werden. Es kann auch passieren, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann oder dass Daten zur Authentisierung im Klartext übermittelt werden. In diesem Fall können Informationen während der Übertragung ausgespäht werden.

2.5. Ausfall von Verzeichnisdiensten

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen können Verzeichnisdienste oder Teile davon ausfallen. Als Folge sind die Daten im Verzeichnis temporär nicht mehr zugänglich. Im Extremfall können auch Daten verloren gehen oder Anmeldungen an vom Verzeichnisdienst bedienten IT-Systemen nicht mehr möglich sein. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

2.6. Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es Angreifenden gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich durchzuführen oder zu umgehen, können sie danach unbefugt auf eine Vielzahl von Daten zugreifen. Somit kann potentiell der gesamte Verzeichnisdienst kompromittiert werden. Dadurch könnte das gesamte betroffene System beeinträchtigt oder gar zerstört werden.

Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzende zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzende zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchzuführen, da Angreifende mehr Zugriffsmöglichkeiten haben, die nur schlecht kontrollierbar sind.

2.7. Fehlerhafte Konfiguration von Verzeichnisdiensten

Verzeichnisdienste verfügen über zahlreiche Funktionen, sodass der Verzeichnisdienst von Anwendenden mit sehr unterschiedlichen Bedürfnissen genutzt werden kann. Eine Fehlkonfiguration dieser zahlreichen Funktionen kann dazu führen, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann. Wenn beispielsweise die Standardkonfiguration nicht ausreichend geprüft und angepasst wird, können die Informationen zur Authentisierung im Klartext oder unzureichend abgesichert übermittelt und damit ausgespäht werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.1 *Allgemeiner Verzeichnisdienst* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.2.1.A1 Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste (B)

Es MUSS eine Sicherheitsrichtlinie für den Verzeichnisdienst erstellt werden. Diese SOLLTE mit dem übergreifenden Sicherheitskonzept der gesamten Institution abgestimmt sein.

APP.2.1.A2 Planung des Einsatzes von Verzeichnisdiensten (B) [Datenschutzbeauftragte, Fachverantwortliche]

Der Einsatz von Verzeichnisdiensten MUSS sorgfältig geplant werden. Die konkrete Nutzung des Verzeichnisdienstes MUSS festgelegt werden. Es MUSS sichergestellt sein, dass der Verzeichnisdienst und alle ihn verwendenden Anwendungen kompatibel sind. Zudem MUSS ein Konzept für eine Struktur aus Objektklassen und Attributtypen entwickelt werden, dass den Ansprüchen der vorgesehenen Nutzungsarten genügt. Bei der Planung eines Verzeichnisdienstes, der personenbezogene Daten beinhaltet, MÜSSEN Personalvertretung und Datenschutzbeauftragte beteiligt werden. Es MUSS ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst entworfen werden. Generell SOLLTE die geplante Verzeichnisdienststruktur vollständig dokumentiert und die Dokumentation bei Änderungen fortgeschrieben werden. Maßnahmen SOLLTEN geplant und umgesetzt werden, die es unterbinden, aus dem Verzeichnisdienst unbefugt Daten sammeln zu können.

APP.2.1.A3 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste (B) [Fachverantwortliche]

Die Administration des Verzeichnisdienstes selbst und die eigentliche Verwaltung der Daten MÜSSEN getrennt werden. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN ausreichend dokumentiert werden.

Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienstbäume MÜSSEN die daraus resultierenden effektiven Rechte kontrolliert werden.

APP.2.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten (B)

Der Verzeichnisdienst MUSS sicher konfiguriert werden. Für die sichere Konfiguration einer Verzeichnisdienste-Infrastruktur MÜSSEN neben dem Server auch die Clients (IT-Systeme und Anwendungen) einbezogen werden.

Wird die Konfiguration des Verzeichnisdienstes oder der mit ihm vernetzten IT-Systeme geändert, SOLLTEN die Benutzenden rechtzeitig über Wartungsarbeiten informiert werden.

APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten (B)

Die Sicherheit des Verzeichnisdienstes MUSS im Betrieb permanent aufrechterhalten werden. Alle den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse SOLLTEN nachvollziehbar dokumentiert und aktuell gehalten werden. Sofern der Verzeichnisdienst zur Verwaltung von Anmeldedaten verwendet wird, MÜSSEN dedizierte Clients bei der Fernwartung eingesetzt werden. Der Zugriff auf alle Administrationswerkzeuge MUSS für normale Benutzende unterbunden werden.

APP.2.1.A17 Absicherung von schutzbedürftigen Anmeldeinformationen (B)

Für Attribute, die schutzbedürftige Anmeldeinformationen wie beispielsweise Passwörter enthalten, MUSS der Zugriff stark eingeschränkt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.2.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A8 Planung einer Partitionierung im Verzeichnisdienst (S)

Sofern eine Partitionierung geplant ist, SOLLTE sich diese an den Schutzzielen des Verzeichnisdienstes orientieren und diese geeignet unterstützen. Eine Partitionierung SOLLTE so geplant werden, dass sie die Schadensauswirkungen bei Sicherheitsvorfällen begrenzt, die unabhängige Administration verschiedener Partitionen ermöglicht und organisatorischen bzw. Sicherheitsgrenzen folgt.

APP.2.1.A9 Geeignete Auswahl von Komponenten für Verzeichnisdienste (S) [Fachverantwortliche]

Für den Einsatz eines Verzeichnisdienstes SOLLTEN geeignete Komponenten identifiziert werden. Es SOLLTE unter Berücksichtigung von APP.6 *Allgemeine Software* ein Anforderungskatalog erstellt werden, nach dem die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden. Im Rahmen der Planung und Konzeption des Verzeichnisdienstes SOLLTEN passend zum Einsatzzweck Anforderungen an dessen Sicherheit formuliert werden. Insbesondere SOLLTE bereits bei der Produktauswahl berücksichtigt werden, wie weitere Sicherheitsanforderungen unter Einsatz der jeweiligen Komponente umgesetzt werden können.

APP.2.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A11 Einrichtung des Zugriffs auf Verzeichnisdienste (S)

Der Zugriff auf den Verzeichnisdienst SOLLTE entsprechend der Sicherheitsrichtlinie konfiguriert werden. Wird der Verzeichnisdienst als Server im Internet eingesetzt, SOLLTE er entsprechend durch ein Sicherheitsgateway geschützt werden.

APP.2.1.A12 Überwachung von Verzeichnisdiensten (S)

Verzeichnisdienste SOLLTEN gemeinsam mit dem Server beobachtet und protokolliert werden, auf dem sie betrieben werden. Insbesondere Änderungen innerhalb des Verzeichnisdienstes sowie Konfigurationsänderungen des Verzeichnisdienstes SOLLTEN vorrangig protokolliert werden.

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten (S)

Werden vertrauliche Informationen übertragen, SOLLTE die gesamte Kommunikation mit dem Verzeichnisdienst über ein sicheres Protokoll entsprechend der Technischen Richtlinie TR-02102 des BSI (z. B. TLS) verschlüsselt werden. Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf.

APP.2.1.A14 Geregelte Außerbetriebnahme eines Verzeichnisdienstes (S) [Fachverantwortliche]

Bei einer Außerbetriebnahme des Verzeichnisdienstes SOLLTE sichergestellt sein, dass weiterhin benötigte Rechte bzw. Informationen in ausreichendem Umfang zur Verfügung stehen. Alle anderen Rechte und Informationen SOLLTEN gelöscht werden. Zudem SOLLTEN die Benutzenden darüber informiert werden, wenn ein Verzeichnisdienst außer Betrieb genommen wird. Bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes SOLLTE darauf geachtet werden, dass dadurch andere Partitionen nicht beeinträchtigt werden.

APP.2.1.A15 Migration von Verzeichnisdiensten (S)

Bei einer geplanten Migration von Verzeichnisdiensten SOLLTE vorab ein Migrationskonzept erstellt werden. In dem Migrationskonzept SOLLTE berücksichtigt werden, ob das Berechtigungsmanagement von altem und neuem Verzeichnisdienst analog funktioniert oder ob neue Berechtigungsstrukturen erforderlich sind. Die Schema-Änderungen, die am Verzeichnisdienst vorgenommen wurden, SOLLTEN vor der Migration analysiert und dokumentiert werden. Weitreichende Berechtigungen, die dazu verwendet wurden, die Migration des Verzeichnisdienstes durchzuführen, SOLLTEN wieder zurückgesetzt werden. Bei der Migration SOLLTE berücksichtigt werden, dass IT-Systeme, die auf den Verzeichnisdienst zugreifen, gegebenenfalls lokale Caches vorhalten oder aus anderen Gründen dort eine Aktualisierung der migrierten Verzeichnisdienstinhalte initiiert werden muss.

APP.2.1.A18 Planung einer Replikation im Verzeichnisdienst (S)

Bei jeder Replikation MUSS festgelegt werden, welches Ziel diese Replikation verfolgt. Dafür SOLLTEN eine Replikationstopologie und -strategie gewählt werden, die zum Ziel bzw. Einsatzszenario passen. Bei Replikationen, die nicht der Hochverfügbarkeit des Dienstes dienen, MUSS der replizierte Inhalt des Verzeichnisdienstes auf die erforderlichen Objekte beschränkt werden. Um die Replikationen zeitgerecht ausführen zu können, SOLLTE eine ausreichende Bandbreite sichergestellt werden.

APP.2.1.A19 Umgang mit anonymen Zugriffen auf Verzeichnisdienste (S)

Sollen anonymen Benutzenden auf einzelne Teilbereiche des Verzeichnisbaums Zugriffe eingeräumt werden, so SOLLTE hierfür ein Proxy-Dienst vorgelagert werden. Dieser Proxy-Dienst SOLLTE über ein gesondertes Konto, einen sogenannten Proxy-User, auf den eigentlichen Verzeichnisdienst zugreifen. Die Zugriffsrechte für diesen Proxy-User SOLLTEN hinreichend restriktiv vergeben werden. Sie SOLLTEN zudem wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird. Damit nicht versehentlich schutzbedürftige Informationen herausgegeben werden, SOLLTE die Suchfunktion des Verzeichnisdienstes dem Einsatzzweck angemessen eingeschränkt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.2.1.A16 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (H)

Im Rahmen der Notfallvorsorge SOLLTE es eine bedarfsgerechte Notfallplanung für Verzeichnisdienste geben. Für den Ausfall wichtiger Verzeichnisdienst-Systeme SOLLTEN Notfallpläne vorliegen. Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten SOLLTEN dokumentiert werden.

APP.2.1.A20 Absicherung der Replikation (H)

Replikationen von vertraulichen Inhalten SOLLTEN zusätzlich zu einer Verschlüsselung auf Applikations- oder Transportebene durch z. B. IPsec gesichert werden. Für die Authentisierung im Rahmen der Replikation SOLLTEN möglichst starke Authentisierungsverfahren verwendet werden.

APP.2.1.A21 Hochverfügbarkeit des Verzeichnisdienstes (H)

Es SOLLTE eine geeignete Strategie zur Hochverfügbarkeit gewählt werden. Hierbei SOLLTE entschieden werden, ob eine Master-Master-Replikation oder Master-Replica-Replikation (früher als Master-Slave-Replikation bezeichnet) geeigneter ist. Es SOLLTEN auch Randbedingungen wie verteilte Standorte oder Verhalten bei Inkonsistenzen berücksichtigt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.2 Active Directory Domain Services

1. Beschreibung

1.1. Einleitung

Active Directory (AD) ist ein Sammelbegriff für verschiedene von Microsoft für Windows Server entwickelte Serverrollen. Die Serverrolle Active Directory Domain Services (AD DS) aggregiert sowohl Funktionalitäten eines Verzeichnis-, als auch Authentifizierungs- und Autorisierungsdienstes sowie einer zentralen Konfigurationsverwaltung für Windows-Infrastrukturen.

Active Directory Domain Services wird hauptsächlich in Netzen eingesetzt, die vorrangig von Microsoft-basierten Betriebssystemen geprägt sind. Ein AD DS speichert und verwaltet Informationen zu Netzressourcen (z. B. Benutzende, Computer und Geräte). Bei Bedarf können diese Informationen, wie in LDAP-Verzeichnisdiensten üblich, auch um anwendungsspezifische Daten erweitert werden. Es dient Anwendenden und Administrierenden dazu, diese Informationen in einer hierarchischen Struktur zu organisieren, bereitzustellen und zu nutzen. Dabei strukturiert AD DS die Objekte in Namensräumen, die als Gesamtstrukturen, Domänen und Organisationseinheiten bezeichnet werden. Eine Gesamtstruktur bildet eine hierarchische Sammlung von Domänen, die jeweils mehrere Organisationseinheiten enthalten können. Die erste und damit in der Hierarchie oben angeordnete Domäne, die in einer Gesamtstruktur angelegt wird, übernimmt systembedingt die Rolle der „Gesamtstruktur Stammdomäne" (englisch „forest root domain") und beinhaltet die administrativen Gruppen, die für gesamtstrukturweite Verwaltungsaufgaben wie beispielsweise das Hinzufügen weiterer Domänen oder Schemaänderungen zuständig sind. Alle Domänen innerhalb einer Gesamtstruktur sind implizit durch bidirektionale, transitive Vertrauensstellungen miteinander verknüpft, so dass die Gesamtstruktur eine logische Sicherheitsgrenze darstellt.

Als Authentisierungsprotokoll nutzt AD DS im Standard Kerberos v5 (in einer durch Microsoft erweiterten Implementierung). Zusätzlich steht weiterhin auch noch das Protokoll NTLM (New Technology LAN Manager) zur Verfügung. NTLM kann dabei einfacher von Angreifenden ausgenutzt werden. Windows Server mit der Serverrolle AD DS werden als Domänencontroller bezeichnet. Aus Verfügbarkeitsgründen werden häufig mehrere Domänencontroller verteilt eingesetzt. Das AD DS bietet außerdem die Möglichkeit eines „Read-Only-Betriebs" eines Domänencontrollers, der für Standorte mit erhöhtem Risiko für die physische Sicherheit vorgesehen ist.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es, Active Directory Domain Services im Regelbetrieb einer Institution abzusichern, die AD DS zur Verwaltung von Windows-Systemen (Client und Server) sowie zur zentralen Authentifizierung und Autorisierung einsetzt.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.2 *Active Directory Domain Services* ist für alle verwendeten Verzeichnisdienste anzuwenden, die auf Microsoft Active Directory Domain Services basieren. Er kann zusätzlich für die Modellierung von Active Directory Lightweight Directory Services (AD LDS), die einen reduzierten Funktionsumfang von AD DS bieten, in Teilen verwendet werden.

In diesem Baustein werden die für Active Directory Domain Services spezifischen Gefährdungen und Anforderungen betrachtet. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten finden sich im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst*. Die dort beschriebenen allgemeinen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt. Dieser Baustein wiederholt nicht die Anforderungen zur Absicherung der Betriebssysteme der Server und Clients, die für den Betrieb und die Verwaltung des AD DS genutzt werden, wie z. B. SYS.1.2.3

Windows Server oder SYS.2.2.3 *Clients unter Windows*. Dieser Baustein geht auch nicht erneut auf die Anforderungen der zugrundeliegenden Netzinfrastruktur ein.

Active Directory Domain Services sollte nicht losgelöst von den Bausteinen ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung,* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration,* OPS.1.2.5 *Fernwartung*, DER.1 *Detektion von sicherheitsrelevanten Ereignissen,* DER.2 *Security Incident Management,* DER.4 *Notfallmanagement* und APP.3.6 *DNS-Server* modelliert werden. Es ist davon auszugehen, dass sich die Anforderungen dieser Bausteine wechselseitig beeinflussen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.2.2 *Active Directory Domain Services* von besonderer Bedeutung.

2.1. Unzureichende Planung der Sicherheitsgrenzen

In AD DS existieren verschiedene Arten von Grenzen. Diese Grenzen definieren die Gesamtstruktur (englisch Forest), die Domäne, die Standorttopologie und die Zuweisung von Rechten. Eine AD-DS-Instanz erzeugt zunächst eine Gesamtstruktur (engl. Forest) als Container auf höchster Ebene für alle Domänen dieser Instanz. Eine Gesamtstruktur kann ein oder mehrere Domänen-Containerobjekte enthalten, die über eine gemeinsame logische Struktur, einen Global Catalog, ein Schema und automatische bidirektionale, transitive Vertrauensbeziehungen verfügen. Dies bedeutet, dass zwischen Domänen innerhalb einer Gesamtstruktur sowohl das Vertrauen zueinander, also auch der Zugriff aufeinander, beidseitig möglich ist. Die Gesamtstruktur stellt also systembedingt die Sicherheitsgrenze dar, innerhalb derer Informationen standardmäßig im AD DS weitergegeben werden. Eine Domäne bildet dabei nur eine Verwaltungsgrenze. Werden Sicherheitsgrenzen nicht entlang der Gesamtstrukturgrenzen realisiert, kann eine Kompromittierung ein höheres Schadensausmaß als erwartet erzeugen, da sie zu einer Kompromittierung aller IT-Systeme in der Gesamtstruktur führen kann. Diese Gefährdung ist eine Besonderheit beim AD DS, da sich die Planung einer Partitionierung im Verzeichnisdienst produktbedingt nicht vollständig umsetzen lässt. Eine vollständige Kompromittierung einer Gesamtstruktur bedeutet, dass Angreifende Kontrolle über alle Objekte, die zu den enthaltenen Domänen gehören, also unter anderem alle Konten und alle IT-Systeme, haben. Damit haben diese potentiell auch Kontrolle über die zugehörigen IT-Systeme und Dienste.

2.2. Zu viele oder nachlässige Vertrauensbeziehungen

Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen ermöglichen es, Konten einer anderen Domäne oder Gesamtstruktur Zugriff auf Ressourcen innerhalb der eigenen Domäne oder Gesamtstruktur zu gewähren. Werden die Vertrauensbeziehungen zwischen Gesamtstrukturen und zwischen Domänen nicht initial und regelmäßig daraufhin evaluiert, ob sie benötigt werden und ob die Sicherheitskontrollen rund um diese Vertrauensbeziehungen ausreichend sind, können Probleme mit Berechtigungen auftreten und Informationen abfließen. Insbesondere wenn die standardmäßig aktive SID-(Security Identifier)-Filterung deaktiviert wird, können komplexe, schwer zu durchschauende Konfigurationsfehler, die zu einer missbräuchlich Nutzung der Vertrauensstellung und zu weitreichenden Zugriffsrechten führen können, auftreten. Gleiches gilt, wenn auf „Selective Authentication" bei Vertrauensbeziehungen zwischen Gesamtstrukturen verzichtet wird.

2.3. Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domänen- und Gesamtstruktur-Funktionsebenen

Bis einschließlich Windows Server 2016 bringt jede neue Generation des Betriebssystems Windows Server zusätzliche Sicherheitsfunktionen und -erweiterungen in Bezug auf AD DS in Form von Domänen- bzw. Gesamtstruktur-Funktionsebenen mit. Werden ältere Betriebssysteme als Domänencontroller bzw. veraltete Domänen- oder Gesamtstruktur-Funktionsebenen eingesetzt, können zeitgemäße Sicherheitsfunktionen nicht genutzt werden. Dies erhöht die Gefahr unsicherer Standardeinstellungen. Eine unsicher konfigurierte Gesamtstruktur oder Domäne gefährdet die darin verarbeiteten Informationen und erleichtert Angriffe durch Dritte.

2.4. Betrieb weiterer Rollen und Dienste auf Domänencontrollern

Werden neben AD DS auf einem Domänencontroller noch weitere Dienste betrieben, erhöht dies, neben den durch AD DS sowieso schon stark kumulierten Diensten, zusätzlich die Angriffsfläche dieser zentralen Komponente durch mögliche zusätzliche Schwachstellen und Fehlkonfigurationen. Solche Dienste können bewusst oder unbewusst missbraucht werden, um z. B. Informationen unberechtigt zu kopieren, zu verändern oder, im Fall von Schwachstellen oder Fehlkonfigurationen, die zur Kompromittierung des Domänencontrollers führen, die Domäne oder Gesamtstruktur zu übernehmen.

2.5. Unzureichende Überwachung und Dokumentation von delegierten Rechten

Wenn die Bildung unternehmensspezifischer Gruppen und die Delegation von Rechten an diese Gruppen- oder an einzelne Benutzendenobjekte nicht systematisch geplant und umgesetzt wird, kann die Delegation nur noch schwer kontrolliert werden. Sie könnte dann etwa viel mehr Zugriffe einräumen als vorgesehen, was durch Dritte missbraucht werden kann. Eine fehlende regelmäßige Auditierung der Zugriffsrechte von Gruppen- und einzelnen Benutzendenobjekte kann das Problem zusätzlich verschärfen. Auch wenn Standardgruppen genutzt und ihre Rechte an eigene Gruppen delegiert werden, etwa bei der Delegation von „Account Operators" / „Konten-Operatoren" an Helpdesk-Mitarbeitende, werden in der Regel mehr Rechte gewährt als tatsächlich benötigt werden.

2.6. Unsichere Authentisierung

Sogenannte „Legacy"- (also historische) Authentisierungsmechanismen im Bereich AD DS wie LAN Manager (LM) und NT LAN Manager (NTLM) v1 sind unsicher und können bei Angriffen unter bestimmten Bedingungen missbraucht werden. Angreifende können beispielsweise ohne Kenntnis der Klartextpasswörter Rechte erhalten und missbrauchen und so Teile der Domäne, die Domäne selbst oder sogar die Gesamtstruktur kompromittieren.

2.7. Zu mächtige oder schwach gesicherte Konten

Anwendungssoftware setzt manchmal Rechte hochprivilegierter Gruppen (beispielsweise von sogenannten *Domänenadministratoren*) für Dienstkonten voraus, um die Produkte einfacher testen und ausbringen zu können, obwohl für den Betrieb deutlich weniger Rechte notwendig sind. Ein besonderes Risiko besteht, wenn diese Dienstkonten mit schwachen Passwörtern gesichert sind. Auch Konten, die nicht Mitglied einer hoch privilegierten Gruppe sind, können administrative Berechtigungen beispielsweise auf einer großen Anzahl von Servern und Clients zugewiesen sein. Damit besitzen sie ähnlich umfangreiche Rechte wie Mitglieder hoch privilegierten Gruppen im AD DS. Die weitreichenden Rechte dieser Konten können von Angreifenden missbraucht werden, um sich in der Domäne weiterzubewegen.

2.8. Nutzung desselben lokalen Administrierendenpassworts auf mehreren IT-Systemen

Auch bei Domänenzugehörigkeit eines IT-Systems ist eine Anmeldung mit lokalen Konten an diesem IT-System weiterhin möglich. Werden dieselben lokalen Anmeldeinformationen auf mehreren IT-Systemen verwendet, kann eine Anmeldung mit diesen unter anderem mit dem lokalen Built-In-Konto *Administrator* auf mehreren IT-Systemen erfolgen. Dies erleichtert Angreifenden die laterale Bewegung und damit die Ausbreitung in der Infrastruktur. Damit steigt das Risiko, dass Angreifende auf einem der IT-Systeme Anmeldeinformationen eines Domänenkontos mit höheren Rechten finden und diese missbrauchen können, um die Domäne und potentiell die Gesamtstruktur zu kompromittieren.

2.9. Unsichere Speicherung von Passwörtern

Die Speicherung der Passwörter erfolgt in der zentralen AD-DS-Datenbank (*ntds.dit*) auf dem Domänencontroller produktbedingt unter anderem mittels MD4-Hashfunktion ohne Salt. Diese Hashfunktion erfüllt nicht die Anforderungen der Technischen Richtlinie TR-02102-1 „Kryptografische Verfahren: Empfehlungen und Schlüssellängen" des BSI. Unautorisierte lesende Zugriffe auf die gespeicherten Passwörter sind daher besonders kritisch. Aufgrund der weiten Verbreitung von AD DS existieren viele Werkzeuge, um die Hashes der Passwörter zu extrahieren. Die AD-DS-Datenbank kann beispielsweise unter Verwendung weiterer auf dem Domänencontroller hinterlegter Schlüssel offline entschlüsselt werden und den Zugriff auf die Hashes ermöglichen. Zudem ist durch die schwache Hashfunktion ein Ermitteln der Klartextpasswörter möglich.

2.10. Unzureichende Absicherung von Domänencontrollern

Jeder (Read-Write)-Domänencontroller einer Domäne hält ein vollständiges Replikat der zentralen AD-DS-Datenbank (*ntds.dit*) vor, in der die Passwörter unsicher gespeichert sind. Neben dem unzureichenden Schutz vor Zugriff durch Dritte auf die Domänencontroller im Betrieb kann auch ein ungeeignetes Backupverfahren zum Abgreifen der zentralen AD-DS-Datenbank und in Folge zum Abfluss von Informationen und der Kompromittierung der Domäne und potentiell der Gesamtstruktur führen. Auch der Betrieb von virtualisierten Domänencontrollern gemeinsam mit weniger schützenswerten virtuellen Maschinen auf einem physischen Virtualisierungshost kann zu einer Kompromittierung des AD DS führen. Dies gilt auch, wenn die administrativen Konten des Virtualisierungshosts, die durch ihre administrativen Tätigkeiten Vollzugriff auf AD DS besitzen, nicht angemessen geschützt werden.

2.11. Hinterlassen von hochprivilegierten Anmeldeinformationen auf Domänenmitgliedsservern und -clients

Erfolgt eine Anmeldung oder Dienstnutzung mit hochprivilegierten Konten auf einem Server oder Client der Domäne, so werden die zugehörigen Anmeldeinformationen auf diesem zwischengespeichert (z. B. im Speicher des Local Security Authority Subsystem / LSASS). Im Fall einer Kompromittierung können Angreifende diese dort extrahieren. Dadurch kann die Kompromittierung eines einzelnen Servers oder Clients der Domäne dazu führen, dass die gesamte Domäne und potentiell die Gesamtstruktur kompromittiert wird.

2.12. Hinzufügen nicht vertrauenswürdiger IT-Systemen zur Windows-Domäne

In den voreingestellten Konfigurationen dürfen alle im AD DS authentifizierten Benutzenden bis zu zehn IT-Systeme zu der Domäne hinzufügen, auch, wenn sie keine administrativen Berechtigungen im AD DS besitzen. Dadurch können sie IT-Systeme in die Domäne hinzufügen, auf denen sie hohe Privilegien besitzen. Diese Privilegien können als Ausgangspunkt für weitere Angriffe verwendet werden. Da das Hinzufügen von IT-Systemen zu einer Domäne eine Verwaltungsaufgabe ist, die typischerweise in einen IT-Prozess eingebettet ist, können hier schwer vorhersehbare Seiteneffekt entstehen, wenn IT-Systeme unkontrolliert der Domäne beitreten, ohne diesen Prozess korrekt zu durchlaufen.

2.13. Vermaschung von administrativen Privilegien durch Integration von weiteren Anwendungen

Werden Anwendungen mit einer Integration in AD DS eingesetzt (beispielsweise Microsoft Exchange), können den durch diese Anwendungen angelegten AD-DS-Konten administrative Berechtigungen in AD DS zugewiesen sein. Dadurch können Sicherheitslücken in diesen Anwendungen dazu führen, dass Angreifende weitreichende Administrationsrechte bei IT-Systemen innerhalb der Gesamtstruktur erhalten. Ein Beispiel hierfür ist die Sicherheitslücke CVE-2019-0686 (PrivExchange) in Microsoft Exchange.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.2 *Active Directory Domain Services* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.2.2.A1 Planung von Active Directory Domain Services (B) [Fachverantwortliche]

Es MUSS eine Funktionsebene für die Domäne(n) und die Gesamtstruktur von mindestens Windows Server 2016 gewählt werden. Ein bedarfsgerechtes Berechtigungskonzept für die Domäne(n) und die Gesamtstruktur MUSS entworfen werden. Dabei MUSS berücksichtigt werden, dass zwischen den einzelnen Domänen einer Gesamtstruktur produktbedingt keine Sicherheitsgrenzen bestehen und daher keine sichere Begrenzung der administrativen Bereiche innerhalb einer Gesamtstruktur möglich ist. Administrative Delegationen MÜSSEN mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet sein. Die geplante Struktur einschließlich etwaiger Schema-Änderungen MUSS nachvollziehbar dokumentiert sein.

APP.2.2.A3 Planung der Gruppenrichtlinien unter Windows (B)

Es MUSS ein Konzept zur Einrichtung von Gruppenrichtlinien vorliegen. Mehrfachüberdeckungen MÜSSEN beim Gruppenrichtlinienkonzept möglichst vermieden werden. In der Dokumentation des Gruppenrichtlinienkonzepts MÜSSEN Ausnahmeregelungen erkannt werden können. Alle Gruppenrichtlinienobjekte MÜSSEN durch restriktive Zugriffsrechte geschützt sein. Für die Parameter in allen Gruppenrichtlinienobjekten MÜSSEN sichere Vorgaben festgelegt sein.

APP.2.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.2.A5 Absicherung des Domänencontrollers (B)

Aufgrund der zentralen Rolle und der Schadensauswirkung bei Kompromittierung des AD DS für die Infrastruktur SOLLTE eine Risikobetrachtung durchgeführt werden. Der Notfallzugriff auf den Domänencontroller mit dem lokalen Restore-Konto DSRM (Directory Services Restore Mode) MUSS im Rahmen des Notfallmanagements geplant werden.

Auf dem Domänencontroller MUSS eine ausreichende Größe für das Sicherheitsprotokoll auf Grundlage des in DER.1 *Detektion von sicherheitsrelevanten Ereignissen* festgelegten Zeitraums eingestellt sein. Aufgrund der zentralen Bedeutung des Domänencontrollers SOLLTEN auf diesem Server keine weiteren Dienste betrieben werden, sofern diese nicht zwingend auf dem *gleichen* Server zum Betrieb des AD DS erforderlich sind.

APP.2.2.A6 Sichere Konfiguration von Vertrauensbeziehungen (B)

Alle Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen MÜSSEN regelmäßig auf ihre Notwendigkeit und Absicherungsmaßnahmen evaluiert werden. Dabei MUSS geprüft werden, ob eine bidirektionale Vertrauensbeziehung notwendig ist. Wenn eine Domäne keine bidirektionale Vertrauensbeziehung zu anderen Domänen in der Gesamtstruktur benötigt, SOLLTE diese Domäne in eine eigene Gesamtstruktur ausgelagert werden, da innerhalb einer Gesamtstruktur produktbedingt keine Anpassung der Vertrauensbeziehungen möglich ist.

Die SID-(Security Identifier)-Filterung bei Vertrauensstellungen zwischen Gesamtstrukturen DARF NICHT deaktiviert werden. Die voreingestellten SIDs DÜRFEN NICHT entfernt werden. Hat der in der Gesamtstruktur abgebildete Informationsverbund, dem vertraut wird, kein ausreichendes Sicherheitsniveau, MUSS für die Vertrauensbeziehung zu dieser Gesamtstruktur „Selective Authentication" verwendet werden.

APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory (B) [Fachverantwortliche]

Es MUSS sichergestellt sein, dass die Konten von Dienste-Administrierenden ausschließlich von Mitgliedern der Gruppe der Dienste-Administrierenden verwaltet werden. Bevor Konten vordefinierten AD-DS-Gruppen hinzugefügt werden, SOLLTE geprüft werden, ob alle der Gruppe zugehörigen Rechte für die mit den Konten verbundenen Tätigkeiten erforderlich sind. Den Gruppen „Schema-Admins" / „Schema-Administratoren" sowie der Gruppe „Enterprise Admins" / „Organisations-Administratoren" und „Domain Admins" / „Domänen-Administratoren" SOLLTEN neben dem AD-DS-Built-In-Konto für Administrierende weitere administrative Konten nur temporär für den Zeitraum zugewiesen werden, in dem sie diese Berechtigungen benötigen.

APP.2.2.A16 Härtung der AD-DS-Konten (B)

Built-in-AD-DS-Konten MÜSSEN mit komplexen Passwörtern versehen werden. Sie DÜRFEN NUR als Notfallkonten dienen. Das Built-in „Guest"- / „Gast"-Konto MUSS deaktiviert werden. Die Berechtigungen für die Gruppe „Everyone" / „Jeder" MUSS beschränkt werden. Privilegierte Konten MÜSSEN Mitglied der Gruppe „Protected Users" / „Geschütze Benutzer" sein. Für Dienstkonten MÜSSEN (Group) Managed Service Accounts verwendet werden. Vor dem Löschen nicht mehr verwendeter Konten MUSS geprüft werden, nach welcher Aufbewahrungsfrist diese gelöscht werden können. Dabei MÜSSEN die Auswirkungen auf die Detektion und gesetzliche Aufbewahrungs- und Löschfristen berücksichtigt werden. Der Zugriff auf das AdminSDHolder-Objekt SOLLTE zum Schutz der Berechtigungen besonders geschützt sein.

APP.2.2.A17 Anmelderestriktionen für hochprivilegierte Konten der Gesamtstruktur auf Clients und Servern (B)

Die Anmeldung von hochpriviligierten Domänen- und Gesamtstruktur-Konten und Gruppen MUSS technisch auf die minimal notwendigen IT-Systeme einschränkt werden. Insbesondere die Anmeldung von Mitgliedern der Gruppen „Schema Admins" / „Schema-Administratoren", „Enterprise Admins" / „Enterprise-Administratoren" und „Domain Admins" / „Domänen-Administratoren" SOLLTE technisch auf den Domänencontroller beschränkt werden, eine Anmeldung an anderen IT-Systemen ist für diese Gruppen also zu unterbinden.

APP.2.2.A18 Einschränken des Hinzufügens neuer Computer-Objekte zur Domäne (B)

Die Berechtigung, in der Domäne neue Computer-Objekte hinzuzufügen, MUSS auf die notwendigen administrativen Konten beschränkt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.2.2.A8 Absicherung des „Sicheren Kanals" (S)

Der „Sichere Kanal" SOLLTE so konfiguriert sein, dass alle übertragenen Daten immer verschlüsselt und signiert werden.

APP.2.2.A9 Schutz der Authentisierung beim Einsatz von AD DS (S)

In der Gesamtstruktur SOLLTE konsequent das Authentisierungsprotokoll Kerberos eingesetzt werden. Dabei SOLLTE für die Absicherung AES128_HMAC_SHA1 oder AES256_HMAC_SHA1 verwendet werden. Wenn aus Kompatibilitätsgründen übergangsweise NTLMv2 eingesetzt wird, SOLLTE die Migration auf Kerberos geplant und terminiert werden. Die LM-Authentisierung und NTLMv1 MÜSSEN deaktiviert sein. Der SMB-Datenverkehr MUSS signiert sein. SMBv1 MUSS deaktiviert sein. Anonyme Zugriffe auf Domänencontroller SOLLTEN unterbunden sein. LDAP-Sitzungen SOLLTEN nur signiert und mit konfiguriertem Channel Binding Token (CBT) erfolgen.

APP.2.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A12 Datensicherung für Domänencontroller (S)

Aufgrund der besonderen Gefährdung der unsicher gespeicherten Passwörter SOLLTE der Zugriff auf die Backups des Domänencontrollers vergleichbar dem Zugriff auf den Domänencontroller selbst abgesichert sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A15 Auslagerung der Administration in eine eigene Gesamtstruktur (H)

Besonders kritische IT-Systeme und Konten zur Administration der Domänen oder der Gesamtstruktur SOLLTEN in eine eigene Gesamtstruktur (häufig als „Red Forest" bezeichnet) ausgegliedert werden, zu der von der zu verwaltenden Gesamtstruktur eine einseitige Vertrauensstellung besteht. Dies SOLLTE im Rahmen des Notfallmanagements bei der Erstellung des Notfallhandbuchs besonders berücksichtigt werden.

APP.2.2.A19 Betrieb von virtualisierten Domänencontrollern (H)

Virtualisierte Domänencontroller SOLLTEN nicht gemeinsam mit weiteren virtuell betriebenen IT-Systemen auf dem gleichen physischen Host betrieben werden. Bei der Absicherung der administrativen Konten für den Zugriff über die Virtualisierungsschicht SOLLTE berücksichtigt werden, dass diese Vollzugriffe auf den Domänencontroller haben und dieser dann vergleichbar mit dem der Gruppe „Domain Admins" / „Domänen-Administratoren" ist. Der Virtualisierungshost, die IT-Systeme, die am Virtualisierungsmanagement beteiligt sind sowie die Administrationskonten für die Virtualisierungsschicht SOLLTEN NICHT zur Gesamtstruktur gehören, zu der der virtualisierte Domänencontroller gehört.

APP.2.2.A20 Trennung von Organisationseinheiten (H)

Organisationseinheiten, die aus IT-Sicherheitsgründen oder sonstigen Gründen Unabhängigkeit voneinander gewährleisten müssen, SOLLTEN sich nicht in der gleichen Gesamtstruktur befinden.

APP.2.2.A21 Konfiguration eines Schichtenmodells (H)

Die Berechtigungsstruktur innerhalb der Gesamtstruktur SOLLTE in Schichten, die sich am Schutzbedarf der Konten, IT-Systeme und Anwendungen orientieren, entworfen werden. Bei dieser Strukturierung SOLLTEN alle Konten, IT-Systeme und Anwendungen innerhalb einer Gesamtstruktur eindeutig einer Schicht zugeordnet werden können. Konten einer höheren Schicht SOLLTEN sich nicht auf Ressourcen einer niedrigeren Schicht anmelden können. Konten einer niedrigeren Schicht SOLLTEN keine Kontrollmöglichkeit über Konten und Ressourcen höherer Schichten besitzen.

APP.2.2.A22 Zeitlich befristete Berechtigungen für die Administration (H)

Konten, die für die Administration verwendet werden, SOLLTEN nur bei Bedarf auf das benötigte Zeitfenster befristet die für die administrative Aufgabe notwendigen Berechtigungen zugewiesen werden.

APP.2.2.A23 Regelmäßige Analyse von Berechtigungen und resultierenden Angriffspfaden (H)

Aufgrund der Komplexität von Berechtigungen, die nicht immer unmittelbar ersichtlich sind, SOLLTE eine regelmäßige Analyse der Berechtigungsstrukturen im AD DS vorgenommen werden. Insbesondere Berechtigungen, die durch die Integration von Anwendungen in AD DS entstehen (beispielsweise Microsoft Exchange) SOLLTEN kritisch auf ihre Notwendigkeit hin geprüft und auf die minimal notwendigen Berechtigungen reduziert werden. Aktualisierungen können ebenfalls auch Berechtigungsstrukturen im AD DS ändern, daher SOLLTE die Analyse auch nach entsprechenden Aktualisierungen durchgeführt werden. Mögliche Angriffspfade über die Berechtigungen der AD-DS-Konten, die beispielsweise bei Kompromittierung von Konten zur Kompromittierung der Domäne bzw. der vollständigen Gesamtstruktur führen, SOLLTEN möglichst gering sein. Die Aktivitäten der verbleibenden, als kritisch identifizierten Konten SOLLTEN besonders überwacht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Website „Active Directory Security“ (https://adsecurity.org) enthält viele weiterführende Informationen zu AD-Sicherheit.

Der Hersteller Microsoft bietet weitergehende Informationen zu Active Directory und dessen Sicherheitsaspekten:

- Einstiegspunkt Active Directory Domain Services https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
- Dokumentation zum „Implementieren von Verwaltungsmodellen der geringsten Rechte“ https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
- Übersicht zu Domänen und Gesamtstrukturen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)
- Sicherheitsaspekte bei Vertrauensstellungen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)
- Dokumentation zum Schichtenmodell https://web.archive.org/web/20171205072455/https:/docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.3 OpenLDAP

1. Beschreibung

1.1. Einleitung

OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Konten, IT-Systeme oder Konfigurationen, in einer standardisierten und definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Kontenverwaltungen, aber auch Konfigurationen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der am meisten verbreiteten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die *Overlays*. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen wie Protokollierung, Replikation und die Wahrung der Integrität verwendet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, auf OpenLDAP basierende Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen geeignet zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.3 *OpenLDAP* ist auf jedes OpenLDAP-Verzeichnis anzuwenden.

In diesem Baustein werden die für OpenLDAP spezifischen Gefährdungen und Anforderungen betrachtet. Dabei wird die Version 2.4 von OpenLDAP zugrunde gelegt. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten gibt es im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst.* Diese müssen zusätzlich berücksichtigt werden. Die dort beschriebenen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt.

OpenLDAP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mitberücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.2.3 *OpenLDAP* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung von OpenLDAP

OpenLDAP kann in Verbindung mit zahlreichen anderen Anwendungen genutzt werden. Diese Anwendungen können auf die Informationen des Verzeichnisdienstes zugreifen und diese in der Regel auch ändern. Wird der Einsatz von OpenLDAP nicht oder unzureichend geplant, können folgende Probleme auftreten:

- Werden die Backends und die zugehörigen Direktiven und Parameter falsch ausgewählt, beeinflussen diese ungewollt die Funktionen, die OpenLDAP anbieten kann. Wird beispielsweise das Backend „back-ldif“ zur Datenspeicherung verwendet, um die Installation einer zusätzlichen Datenbank zu umgehen, stehen nur rudimentäre

Funktionen des Verzeichnisdienstes zur Verfügung. Eine große Menge von Benutzenden oder anderen Objekten kann dann nicht geeignet verwaltet werden.

- Wenn der Einsatz von Overlays mangelhaft geplant wird, können in OpenLDAP nicht benötigte Operationen ausgeführt oder sonstige Funktionen beeinträchtigt werden. Beispielsweise werden Zugriffe auf den Verzeichnisdienst nicht oder falsch protokolliert, wenn die Debug-Funktion des slapd-Servers selbst und die Overlays „auditlog" und „accesslog" unzureichend geplant werden.
- OpenLDAP kann in einer ungeeigneten Systemumgebung ausgeführt werden. Wird ein verteiltes Dateisystem wie Network File System (NFS) verwendet, um die OpenLDAP-Daten abzuspeichern, könnten Dateifunktionen von OpenLDAP nicht verwendet werden. Ein Beispiel dafür ist die von vielen Datenbanken verwendete Locking-Funktion, die es ermöglicht, die Datenbank des Verzeichnisdienstes zu sperren, wenn mehrere Benutzende parallel schreibend auf die Datenbank zugreifen möchten.
- Es könnten inkompatible Versionen einer oder mehrerer Anwendungen auf die von OpenLDAP verwendeten Datenbanken zugreifen. Beispielsweise werden die Spezifikationen des Protokolls LDAPv3 nicht von OpenLDAP ohne zusätzliche Erweiterungen erfüllt. Zudem können auch Verbindungsprobleme mit den Anwendungen entstehen, wenn die falsche Version eines oder mehrerer Programme eingesetzt wird, die mit OpenLDAP nicht kompatibel sind.

2.2. Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP

Auf die durch OpenLDAP verwalteten Daten (Objekte im Verzeichnisdienst ebenso wie Konfigurationseinstellungen) kann über verschiedene Möglichkeiten zugegriffen werden. Die Offline- und Online-Zugriffe erfüllen dabei ganz oder teilweise identische Funktionen. Bei einem Online-Zugriff wird über das Protokoll LDAP und den slapd auf die Daten zugegriffen. Beim Offline-Zugriff wird direkt auf die Datenbankdateien zugegriffen, bzw. es wird ein ldif-Export des Verzeichnisses editiert und anschließend wieder zurück in die Datenbank geladen. Werden diese Möglichkeiten vermischt oder wird die jeweilige Wirkungsweise vom Offline- oder Online-Zugriff fehlinterpretiert, können zahlreiche Fehler auftreten. In der Folge ist die resultierende Datenbank für OpenLDAP inkonsistent und kann somit nicht mehr fehlerfrei genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.3 *OpenLDAP* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.2.3.A1 Planung und Auswahl von Backends und Overlays für OpenLDAP (B)

Der Einsatz von OpenLDAP in einer Institution MUSS sorgfältig geplant werden. Soll OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden, so MÜSSEN die Planung, Konfiguration und Installation der Anwendungen mit OpenLDAP aufeinander abgestimmt werden. Für die zur Datenhaltung verwendete Datenbank MUSS

sichergestellt werden, dass die verwendete Version kompatibel ist. Backends und Overlays für OpenLDAP MÜSSEN restriktiv selektiert werden. Dazu MUSS sichergestellt werden, dass die OpenLDAP-Overlays in der korrekten Reihenfolge eingesetzt werden. Bei der Planung von OpenLDAP MÜSSEN die auszuwählenden und unterstützten Client-Anwendungen berücksichtigt werden.

APP.2.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.3.A3 Sichere Konfiguration von OpenLDAP (B)

Für die sichere Konfiguration von OpenLDAP MUSS der slapd-Server korrekt konfiguriert werden. Es MÜSSEN auch die verwendeten Client-Anwendungen sicher konfiguriert werden. Bei der Konfiguration von OpenLDAP MUSS darauf geachtet werden, dass im Betriebssystem die Berechtigungen korrekt gesetzt sind. Die Vorgabewerte aller relevanten Konfigurationsdirektiven von OpenLDAP MÜSSEN geprüft und gegebenenfalls angepasst werden. Die Backends und Overlays von OpenLDAP MÜSSEN in die Konfiguration einbezogen werden. Für die Suche innerhalb von OpenLDAP MÜSSEN angemessene Zeit- und Größenbeschränkungen festgelegt werden. Die Konfiguration am slapd-Server MUSS nach jeder Änderung geprüft werden.

APP.2.3.A4 Konfiguration der durch OpenLDAP verwendeten Datenbank (B)

Die Zugriffsrechte für neu angelegte Datenbankdateien MÜSSEN auf die Kennung beschränkt werden, in deren Kontext der slapd-Server betrieben wird. Die Standard-Einstellungen der von OpenLDAP genutzten Datenbank MÜSSEN angepasst werden.

APP.2.3.A5 Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP (B)

Die in OpenLDAP geführten globalen und datenbankspezifischen Zugriffskontrolllisten (Access Control Lists) MÜSSEN beim Einsatz von OpenLDAP korrekt berücksichtigt werden. Datenbank-Direktiven MÜSSEN Vorrang vor globalen Direktiven haben.

APP.2.3.A6 Sichere Authentisierung gegenüber OpenLDAP (B)

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzenden unterscheiden soll, MÜSSEN sich diese geeignet authentisieren. Die Authentisierung zwischen dem slapd-Server und den Kommunikationsbeteiligten MUSS verschlüsselt werden. Es SOLLTEN nur die Hashwerte von Passwörtern auf den Clients und Servern abgespeichert werden. Es MUSS ein geeigneter Hashing-Algorithmus verwendet werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.2.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A8 Einschränkungen von Attributen bei OpenLDAP (S)

Anhand von Overlays SOLLTEN die Attribute in OpenLDAP eingeschränkt werden. OpenLDAP SOLLTE so angepasst werden, dass Werte im Verzeichnisdienst nur einem bestimmten regulären Ausdruck entsprechen. Zudem SOLLTE mit Hilfe von Overlays sichergestellt werden, das ausgesuchte Werte nur einmal im Verzeichnisbaum vorhanden sind. Solche Restriktionen SOLLTEN ausschließlich auf Daten von Nutzenden angewendet werden.

APP.2.3.A9 Partitionierung und Replikation bei OpenLDAP (S)

Bei einer Partitionierung oder Replikation von OpenLDAP SOLLTE die Aufteilung geeignet für die Sicherheitsziele ausgewählt werden. Dabei SOLLTEN Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Ein Replikationsmodus SOLLTE in Abhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen gewählt werden.

APP.2.3.A10 Sichere Aktualisierung von OpenLDAP (S)

Bei Updates SOLLTE darauf geachtet werden, ob die Änderungen eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Beim Update auf neue Releases SOLLTE geprüft werden, ob die verwendeten Overlays und Backends in der neuen Version weiterhin zur Verfügung stehen. Ist dies nicht der Fall, SOLLTEN geeignete Migrationspfade ausgewählt werden.

Setzen Administrierende eigene Skripte ein, SOLLTEN sie daraufhin überprüft werden, ob sie mit der aktualisierten Version von OpenLDAP problemlos zusammenarbeiten. Die Konfiguration und die Zugriffsrechte SOLLTEN nach einer Aktualisierung sorgfältig geprüft werden.

APP.2.3.A11 Einschränkung der OpenLDAP-Laufzeitumgebung (S)

Die Laufzeitumgebung des slapd-Servers SOLLTE, möglichst mit Mitteln des Betriebssystems, auf die minimal benötigten Dateien, Verzeichnisse und vom Betriebssystem bereitgestellten Funktionen eingeschränkt werden. Werden hierfür Containerisierungstechniken eingesetzt, SOLLTEN diese unter Berücksichtigung von SYS.1.6 *Containerisierung* genutzt werden. Wird der slapd-Server als exklusiver Dienst auf einem dedizierten Server betrieben, SOLLTE dieser ausreichend gehärtet sein.

APP.2.3.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.3 *OpenLDAP* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.1 Webanwendungen und Webservices

1. Beschreibung

1.1. Einleitung

Webanwendungen bieten bestimmte Funktionen und dynamische (sich verändernde) Inhalte. Dazu nutzen Webanwendungen die Internetprotokolle HTTP (Hypertext Transfer Protocol) oder HTTPS. Bei HTTPS wird die Verbindung durch das Protokoll TLS (Transport Layer Security) kryptografisch abgesichert. Webanwendungen stellen auf einem Server Dokumente und Bedienoberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, wie z. B. an Webbrowser.

Webservices sind Anwendungen, die das HTTP(S)-Protokoll verwenden, um Daten für andere Anwendungen bereitzustellen. In der Regel werden sie nicht unmittelbar durch Benutzende angesteuert.

Um eine Webanwendung oder einen Webservice zu betreiben, sind in der Regel mehrere Komponenten notwendig. Üblich sind Webserver, um Daten auszuliefern und Applikationsserver, um die eigentliche Anwendung oder den Webservice zu betreiben. Außerdem werden zusätzliche Hintergrundsysteme benötigt, die oft als Datenquellen über unterschiedliche Schnittstellen angebunden sind, z. B. Datenbanken oder Verzeichnisdienste.

Webanwendungen und Webservices werden sowohl in öffentlichen Datennetzen als auch in lokalen Netzen einer Institution (Intranet) eingesetzt, um Daten und Anwendungen bereitzustellen. In der Regel müssen sich Clients authentisieren, um auf eine Webanwendung oder einen Webservice zugreifen zu können.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Webanwendungen und Webservices sicher einzusetzen sowie Informationen zu schützen, die durch sie verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jede Webanwendung und jeden Webservice anzuwenden, die im Informationsverbund eingesetzt werden.

Anforderungen an Webserver und an die redaktionelle Planung eines Webauftritts werden in diesem Baustein nicht behandelt. Sie sind im Baustein APP.3.2 *Webserver* zu finden. Die Entwicklung von Webanwendungen wird im Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.

Webservice-Schnittstellen werden oft via Representational State Transfer (REST) und Simple Object Access Protocol (SOAP) realisiert. In diesem Baustein werden nur REST-basierte Webservices betrachten. Der Fokus liegt dabei auf der Lebenszyklusphase „Betrieb". Sicherheitsanforderungen, die sich beispielsweise aus der Planung und Konzeption sowie Aussonderung und Notfallvorsorge ergeben, werden in diesem Baustein nicht betrachtet, sondern müssen gesondert im Rahmen einer Risikoanalyse ermittelt werden.

Allgemeine Anforderungen an die Auswahl von Software werden im Baustein APP.6 *Allgemeine Software* betrachtet.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.1 *Webanwendungen und Webservices* von besonderer Bedeutung.

2.1. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung oder dem Webservice unzureichend protokolliert werden, können diese unter Umständen zu einem späteren Zeitpunkt nur schwer nachvollzogen werden. Die Ursachen für ein Ereignis sind dann möglicherweise nicht mehr ermittelbar. So können z. B. kritische Fehler oder unerlaubte Änderungen in der Konfiguration der Webanwendung übersehen werden.

2.2. Offenlegung sicherheitsrelevanter Informationen bei Webanwendungen und Webservices

Webseiten und Daten, die von einer Webanwendung oder einem Webservice generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es bei Angriffen erleichtern, gezielt Webanwendungen oder Webservices anzugreifen.

2.3. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung oder eines Webservices automatisiert genutzt werden, können so zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann so z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem kann eine Liste mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung oder der Webservice Informationen über vorhandene Konten zurück gibt. Darüber hinaus können wiederholte Aufrufe von ressourcenintensiven Funktionen wie z. B. komplexen Datenbankabfragen für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.

2.4. Unzureichende Authentisierung

Oft sollen spezielle Funktionen einer Webanwendung oder eines Webservices nur bestimmten Gruppen vorbehalten bleiben. Die entsprechenden Personen erhalten dann z. B. Konten, die exklusiv mit den notwendigen Zugriffsrechten ausgestattet sind. Unter diesen Konten authentisieren sich die Benutzenden zu Beginn jeder Sitzung in der Webanwendung oder dem Webservice, z. B. mit Kontoname und Passwort. Wird diese Authentisierung nicht korrekt konfiguriert, kann sie möglicherweise umgangen werden. Außerdem kann eine Webanwendung oder ein Webservice so konfiguriert werden, dass Zugangsdaten auf dem Webserver unsicher gespeichert werden. Im Falle eines erfolgreichen Angriffs verfügen Angreifende dann über große Mengen von Zugangsdaten, die sie auch an anderen Stellen einsetzen könnten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.1 *Webanwendungen und Webservice* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Beschaffungsstelle

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.